UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* SEIZURE WARRANT FOR BLOCKFI LENDING LLC ACCOUNT #OFEC57F9 BELONGING TO CHRISTOPHER VOLDEN	)	Case No. 2:21-mj-573

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
BlockFi Lending LLC account #Ofec57f9

located in the Southern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:
BlockFi Lending LLC account #Ofec57f9

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☐ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841	To manufacture, distribute, or dispense a controlled substance
21 U.S.C. § 846	Conspiracy to distribute and possess with intent to distribute, controlled substances, including distribution by means of the Internet

The application is based on these facts:

See attached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

TFO
Applicant's signature

Andrew Wuertz, DEA Task Force Officer
Printed name and title

Sworn to before me and signed in my presence.

Date: September 1, 2021

City and state: Columbus, OH

Kimberly A. Johnson
United States Magistrate Judge

AFFIDAVIT IN SUPPORT OF APPLICATIONS FOR SEIZURE WARRANTS

I, Andrew Wuertz, being duly sworn under oath, depose and say:

INTRODUCTION

1. I am a Task Force Officer with the DEA and have been since May of 2010. I am assigned to the Central Ohio Cyber Drug Task Force (COCDTF) in Columbus, Ohio, where I am is responsible for conducting narcotics investigations involving dark web marketplaces. Prior to becoming a Task Force Officer, I have been employed as an Upper Arlington Police Officer for 24 years. While working with the DEA, I was assigned to the COCDTF with other law enforcement agencies targeting drug and weapon shipments purchased off the internet. As a Task Force Officer, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. Since working with the DEA, I have been involved in narcotics-related arrests, executed search warrants that resulted in the seizure of narcotics, and participated in narcotics investigations. Through training and experience, I am familiar with the manner in which persons involved in the illicit distribution of controlled substances often operate. In particular, I am aware that drug traffickers often communicate with their customers, couriers, and/or associates through the use of standard hardline telephones, and cellular telephones, or use of multiple telephones or other devices, to avoid detection by law enforcement.

2. Based on my training, experience, and participation in drug trafficking and computer-related investigations, I know and have observed the following:

a. I have learned about the manner in which individuals and organizations distribute controlled substances throughout the United States;

b. I know drug traffickers often purchase and/or title assets in fictitious names, aliases or the names of relatives, associates, or business entities to avoid detection of these assets by government agencies. I know that even though these assets are in the names other than the drug traffickers, the drug traffickers actually own and continue to use these assets and exercise dominion and control over them;

c. I know drug traffickers must maintain on-hand large amounts of crypto-currency and U.S. currency to include stored in financial accounts readily accessible in order to maintain and finance their ongoing drug business;

d. I know when drug traffickers amass large proceeds from the sale of drugs, the drug traffickers attempt to legitimize these profits through money laundering activities. To accomplish these goals, drug traffickers utilize the following methods, including, but not limited to: domestic and international banks and their attendant services, securities brokers, professionals such as attorneys and accountants, casinos, real estate, shell corporations and business fronts and otherwise legitimate businesses which generate large quantities of currency; and

e. I know that Bitcoin and other crypto currency accounts are often times used by drug traffickers to launder money or conceal drug proceeds because of the anonymity associated with the use of Bitcoin and other crypto currency accounts and because crypto currency is decentralized.

PURPOSE OF AFFIDAVIT

3. This affidavit is submitted in support of an application for a combined criminal and civil forfeiture seizure warrant for all funds and digital currencies in the following BlockFi Lending LLC account:

a. All remaining funds—including cryptocurrencies—stored in the BlockFi account belonging to Christopher VOLDEN.

(collectively, hereafter, the "SUBJECT ACCOUNT").

4. As set forth below, I submit that there is probable cause to believe that the SUBJECT ACCOUNT is property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of violations of 21 U.S.C. § 841 (To manufacture, distribute, or dispense a controlled substance) and 21 U.S.C. § 846 (conspiracy to distribute and possess with intent to distribute, controlled substances, including distribution by means of the Internet). The SUBJECT ACCOUNT is therefore subject to forfeiture to the United States under 21 U.S.C. § 853.

5. I further submit that there is probable cause to believe that the SUBJECT ACCOUNT constitutes (1) moneys, negotiable instruments, securities, or other things of value furnished or intended to be furnished in exchange for a controlled substance, in violation of the Controlled Substances Act ("CSA"); (2) proceeds traceable to such an exchange; or (3) moneys, negotiable instruments, or securities used or intended to be used to facilitate a violation of the CSA. The SUBJECT ACCOUNT is therefore subject to forfeiture to the United States under 21 U.S.C. § 881(a)(6).

6. Additionally, there is probable cause to believe that the SUBJECT ACCOUNT constitutes property involved in a money laundering transaction or money laundering conspiracy, in violation of 18 U.S.C. § 1956, or are traceable to such property. The SUBJECT ACCOUNT is, therefore, subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1) (civil forfeiture) and 982(a)(1) (criminal forfeiture).

7. Because this affidavit is submitted for the limited purpose of obtaining warrants authorizing the seizure of the SUBJECT ACCOUNT, I am not including every fact known to me about DEFENDANT or the larger investigation.

8. This affidavit is based upon my own personal observations, my training and experience, discussions with other agents who are familiar with this investigation, and information collected during this investigation through, among other things, witness interviews, law enforcement investigation reports, information obtained through searches, and public records.

FORFEITURE AND SEIZURE AUTHORITY

9. As to civil forfeiture, under 21 U.S.C. § 881(a), "[t]he following shall be subject to forfeiture to the United States and no property right shall exist in them: . . . (6) All moneys, negotiable instruments, securities, or other things of value furnished or intended to be furnished by any person in exchange for a controlled substance or listed chemical in violation of this subchapter, all proceeds traceable to such an exchange, and all moneys, negotiable instruments, and securities used or intended to be used to facilitate any violation of this subchapter." Property subject to civil forfeiture under 21 U.S.C. § 881(a) may be seized pursuant to 18 U.S.C. § 981(b) (by 21 U.S.C. § 881(b)). Under 18 U.S.C. § 981(a)(1)(A), "[a]ny property, real or personal, involved in a transaction in violation of [18 U.S.C. §§ 1956], or any property traceable to such property" is subject to forfeiture to the United States. Property subject to civil forfeiture under 18 U.S.C. § 981(a)(1) may be seized pursuant to 18 U.S.C. § 981(b).

10. As to criminal forfeiture, under 21 U.S.C. § 853(a), "[a]ny person convicted of a violation of this subchapter or subchapter II of this chapter punishable by imprisonment for

more than one year shall forfeit to the United States, irrespective of any provision of State law [*inter alia*]—(1) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; [and] (2) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation." As property subject to criminal forfeiture under 21 U.S.C. § 853(a), the SUBJECT ACCOUNT may be seized pursuant to 21 U.S.C. § 853(f). Under 21 U.S.C. § 970, Section 853 applies in every respect to a violation of this subchapter punishable by imprisonment for more than one year, including violations of 21 U.S.C. § 963.

11. Under 18 U.S.C. § 982(a)(1), "[t]he court, in imposing sentence on a person convicted of an offense in violation of 18 U.S.C. §§ 1956 shall order that the person forfeit to the United States any property, real or personal, involved in such offense, or any property traceable to such property." As property subject to criminal forfeiture under 18 U.S.C. § 982(a)(1), the SUBJECT ACCOUNT may be seized pursuant to 21 U.S.C. § 853(f) (by 18 U.S.C. § 982(b)(1).

12. With respect to seizure, 21 U.S.C. § 853(f) specifically provides that a court may issue a criminal seizure warrant when it "determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that a[] [protective] order under [21 U.S.C. § 853(e)] may not be sufficient to assure the availability of the property for forfeiture." As set forth further below, there is a substantial risk that the SUBJECT ACCOUNT will be withdrawn, moved, dissipated, or otherwise become unavailable for forfeiture unless immediate steps are taken to secure them. As a form of cryptocurrency, the SUBJECT ACCOUNT is inherently portable and fungible. I therefore

submit that a protective order under 21 U.S.C. § 853(e) would not be sufficient to assure that the SUBJECT ACCOUNT will remain available for forfeiture.

13. Furthermore, pursuant to 18 U.S.C. § 981(b)(3), "[n]otwithstanding the provisions of rule 41(a) of the Federal Rules of Criminal Procedure, a seizure warrant may be issued pursuant to this subsection by a judicial officer in any district in which a forfeiture action against the property may be filed under section 1355(b) of title 28, and may be executed in any district in which the property is found, or transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement."

14. For the reasons listed above, the United States seeks a combined criminal and civil seizure warrant, authorizing law enforcement to seize the SUBJECT ACCOUNT and preserve it pending further forfeiture proceedings.

BACKGROUND ON THE DARK WEB & CRYPTOCURRENCY

15. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

a. The "dark web" is a portion of the "deep web[1]" of the Internet, where individuals must use an anonymizing software or application called a "darknet" to access content and websites. Within the dark web, criminal marketplaces operate, allowing individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet (sometimes called the "clear web" or simply the "web"). These online market websites use a variety of technologies, including the Tor network (defined below) and other encryption

[1] The deep web is the portion of the Internet not indexed by search engines. Examples are databases and internal networks belonging to private industry, government agencies, or academic institutions.

technologies, to ensure that communications and transactions are shielded from interception and monitoring. Famous dark web marketplaces ("DWM's"), also called Hidden Services, such as Silk Road 1, Silk Road 2, AlphaBay, and Hansa (all of which have since been shut down by law enforcement), operated similarly to clear web commercial websites such as Amazon and eBay, but offered illicit goods and services. When law enforcement shut down the four DWM's listed above, they also obtained images of their servers, and law enforcement has been able to mine the data from those sites for information about the customers and vendors who used them.

b. "Vendors" are the dark web's sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of "vendor accounts" on dark web marketplaces. Customers, meanwhile, operate "customer accounts." Vendor and customer accounts are not identified by numbers, but rather monikers or "handles," much like the username one would use on a clear web site. If a moniker on a particular marketplace has not already been registered by another user, vendors and customers can use the same moniker across multiple marketplaces, and based on seller and customer reviews, can become well known as "trusted" vendors or customers. It is also possible for the same person to operate multiple customer accounts and multiple vendor accounts at the same time. For example, based on my training and experience, I know that one person could have a vendor account that he or she uses to sell illegal goods on a dark web marketplace in exchange for cryptocurrency; that same vendor could also have a different customer account that he or she uses to exchange cryptocurrency earned from vendor sales

for fiat currency[2]. Because they are separate accounts, a person could use different accounts to send and receive the same cryptocurrency on the dark web. I know from training and experience that one of the reasons dark web vendors have multiple monikers for different vendor and customer accounts, is to prevent law enforcement from identifying which accounts belong to the same person, and who the actual person is that owns or uses the accounts.

c. The "Tor network," or simply "Tor" (an abbreviation for "The Onion Router"), is a special network of computers on the Internet, distributed around the world, designed to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor also enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network. Such hidden services operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software, including a browser known as "Tor Browser," designed to access the Tor network. Examples of hidden services websites are the aforementioned AlphaBay and Hansa. Tor is available on cellphones using the Android and Apple operating systems by installing an application that puts a TOR-enabled internet browser on a user's cellphone, which then routes the phone's IP address through different servers all over the world, making it extremely difficult to track.

---

[2] Fiat currency is currency created and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

d. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[3] Cryptocurrency is not illegal in the United States.

e. Bitcoin[4] ("BTC") is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by "mining."

---

[3] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

[4] Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

An individual can "mine" bitcoins by using his/her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it's not completely anonymous, Bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and credit systems.

f. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key.") A public address is represented as a case-sensitive string of letters and numbers, 26–25 (35) characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key - the cryptographic equivalent of a password or PIN - needed to access the address. Only the

holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

g. Although cryptocurrencies such as Bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an oft-used means of payment for illegal goods and services on hidden services websites operating on the Tor network. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the dark web marketplaces. As of April 1, 2021, one bitcoin is worth approximately $59,000.00, though the value of bitcoin is generally much more volatile than that of fiat currencies.

h. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR

code[5] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

i. Bitcoin "exchangers" and "exchanges" are individuals or companies that exchange bitcoin for other currencies, including U.S. dollars. According to the Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.[6] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone

[5] A QR code is a matrix barcode that is a machine-readable optical label.

[6] *See* "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," *available at* https://www.fincen.gov/resources/statutes-regulations/guiadance/application-fincens-regulations-persons-administering.

number, and/or the full bank account and routing numbers that the customer links to his/her exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who not only lack AML or KYC protocols but often advertise their ability to offer customers stealth and anonymity. These illicit exchangers often exchange fiat currency for cryptocurrencies, such as by meeting customers in person or by shipping fiat currency through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9-10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1-2%).

j. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), investigators may be able to use the recovery seed phrase to recover or

reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

PROBABLE CAUSE STATEMENT

SUMMARY OF THE INVESTIGATION

16. In early December, 2019, investigators from the Central Ohio Cyber Drug Task Force (COCDTF) identified a dark web drug vendor operating under the moniker "INSTRUMENT." Information gathered from the dark web indicated that "INSTRUMENT" was active on several marketplaces advertising sales of various controlled substances that would be shipped to and from the United States. Investigators learned that in July of 2019, a drug task force in Sacramento, California, made an undercover (UC) purchase over the dark web from "INSTRUMENT" of approximately one gram of methylenedioxy-methamphetamine (MDMA).

17. Between December 2019 and May 2020, COCDTF investigators in Columbus, Ohio, made four UC purchases off the dark web marketplace "Empire" from "INSTRUMENT." The purchases included 25 dosage units of lysergic acid diethylamide (LSD) on December 12, 2019; five grams of MDMA on December 22, 2019; five dosage units of LSD on April 23, 2020; and five grams of MDMA on May 4, 2020. Each order took approximately one week to arrive in Columbus, and were sent via United States Postal Service (USPS) from different return addresses in the Minneapolis/St.Paul, Minnesota area.

18. In February of 2021, while conducting blockchain analysis on seized market place data associated with "INSTRUMENT," COCDTF investigators identified 127 transactions originating in INSTRUMENT's dark web vendor wallets that were sent to BitPay.com.

19. On February 26, 2021, COCDTF investigators sent a subpoena to Subpoenas@BitPay.com requesting all information associated with the transactions. On March 11, 2021, BitPay responded with a spreadsheet identifying 129 transactions, consisting of a total of 95.371032 bitcoin valued at approximately $43,400.11 at the time of the transactions. The spreadsheet identified the following transactions:

- Five transactions between March 9, 2014 through April 18, 2014 for approximately $6,693.96 sent to BtcTrip, a website that is no longer in existence, but a clear web search indicates it was a website designed to allow users to buy plane tickets using bitcoin.

- 105 transactions between February 24, 2014 through March 28, 2015 for approximately $24,592.62 sent to Gyft Inc., a website that allows you to buy, send, and redeem gift cards for over 200 different retailers.

- One transaction on December 07, 2014 for approximately $35.01 sent to Namecheap.com, a website that allows users to buy internet domains (website addresses).

- 17 transactions between April 29, 2014 through June 17, 2014 for approximately $12,067.56 sent to SnapCard, which allowed users to pay with bitcoin at online retailers that don't officially accept cryptocurrency. The company has since been purchased by Wyre, a payment service.

- One transaction on July 8, 2014 for approximately $10.96 sent to Warner Bros. Records. The transaction had a buyer's email address listed as Chris.Volden@gmail.com.

20. On March 15, 2021, investigators sent a subpoena to LegalPapers@Fiserv.com regarding any information on the 105 transactions conducted on Bitpay.com to Gyft, Inc. On April 6, 2021 Fiserv responded with a spreadsheet identifying 165 transactions, worth

approximately $33,113.37, belonging to the same user account, identified by Gyft ID 76900276-6043-4ce8-89b0-d9211aa90090. The account listed three email addresses, Chris.Volden@gmail.com, Chris@bellslabradors.com, and Zaneisgreat@lelantos.org. All gift cards purchased were marked "self-gifted" and for big box retailers, restaurants and entertainment services. Investigators know it is common for Darknet Vendors to cash out their bitcoin in the form Gift Cards to avoid detection and report requirements from banks and law enforcement. Gyft, Inc. also listed the IP Addresses used during each transaction. A search of the IP address locations shows the transactions were conducted in, Saint Paul, Minnesota; Chicago, Illinois; Volin, South Dakota; and New York, New York; with the majority being conducted in Saint Paul, Minnesota.

21. A law enforcement database search of the email address Chris.Volden@gmail.com identified the user as Christopher Bryan VOLDEN with a date of birth of July 1, 1985. A public records check of VOLDEN listed his address as 4733 Bouleau Road, White Bear Lake, Minnesota, a suburb of Saint Paul. The prior UC drug buys from INSTRUMENT revealed all the packages were shipped from the Minneapolis/Saint Paul, Minnesota area.

22. Investigators also learned from Homeland Security Investigations (HSI) New York that VOLDEN was being investigated in 2013 for selling bitcoin to a known dark web market vendor on the marketplace "Silk Road." At the time, HSI New York identified VOLDEN's moniker as POLYGAMUS and POLYGAMUZ. A U.S. Customs and Border Protection Database query revealed VOLDEN was the subject of three seizures, including 17.5 grams of LSD in 2016, 3.3 grams of cocaine in 2013, and 107 grams of MDMA in 2013.

23. Investigators also learned that on February 19, 2013, VOLDEN was arrested by Saint Paul Police Department (SPPD) for selling synthetic narcotics. VOLDEN admitted to SPPD that he and his girlfriend, Angela WHEELER, sold numerous controlled substance over the internet, specifically on "Silk Road" marketplace. VOLDEN explained that he had started the business and made the initial orders of their products, and WHEELER often helped him by sending/receiving orders of controlled substances through the mail. A check of VOLDEN's criminal history confirmed the SPPD arrest, but not a conviction. Investigators believe VOLDEN or WHEELER switched the dark web moniker from POLYGAMUS to INSTRUMENT after the arrest.

24. On May 6, 2021, COCDTF investigators sought and received authorization for a federal search warrant on the Google account Chris.Volden@gmail.com. On May 11, 2021, Google provided the requested information associated with that account. While analyzing the records from Google, COCDTF investigators identified various other email addresses in contact with VOLDEN, including Wheelera66@gmail.com. In VOLDEN's account, Wheelera66@gmail.com is attributed to Angela WHEELER, his known girlfriend. Also, in a Google chat that took place on March 28, 2021, the user of Wheelera66@gmail.com identified themselves as Angela WHEELER.

25. Later in May 2021, COCDTF investigators made two additional UC purchases off the dark web marketplace "White House Market" from "INSTRUMENT." The purchases included 10 dosage units of LSD on May 11, 2021; and 50 dosage units of LSD on May 20, 2021. Following the May 11 purchase, investigators on surveillance followed VOLDEN to a United States Postal Service (USPS) drop box, and recovered an envelope with the same shipping address in Columbus that was used during the UC transaction. The envelope was photographed,

repackaged, and forwarded to COCDTF investigators in Columbus. Also recovered from the same USPS drop box were thirteen (13) other envelopes matching the envelope from the UC purchase. Those envelopes were addressed to different names and addresses in multiple states including New York, Georgia, Florida, Colorado, Alabama, Oregon, Pennsylvania, Oklahoma, and other states. All of the envelopes had the same or a similar return address that the UC purchase letter had printed on it. Following the May 20 purchase, investigators on surveillance saw VOLDEN and WHEELER leave their home together in the late afternoon, but did not see them stop at a USPS drop box and were unable retrieve an envelope. COCDTF investigators, however, received the order in Columbus on May 26, 2021, that was post marked in Saint Paul, Minnesota, by USPS on May 20, 2021. USPIS investigators advised COCDTF investigators that the letter would have had to have been mailed before 6:00 PM CST on May 20 in order to be post marked on May 20. COCDTF investigators believe VOLDEN and WHEELER dropped the order in a mailbox when they were together and out of view of investigators on surveillance.

26. Law enforcement sources in Minnesota confirmed for investigators that neither VOLDEN nor WHEELER have any known employment history for the last five years. However, in the search warrant information for VOLDEN's Google account, there were documents indicating VOLDEN paid approximately $578,000.00 in March 2021 for the home he shares with WHEELER.

27. On June 9, 2021, COCDTF investigators learned that VOLDEN and WHEELER would be traveling to Mexico with plans to leave on June 12, 2021. An update to the "INSTRUMENT" vendor profile on White House Market appeared on June 10, 2021, stating, "Gone fishing. I will return with a fully stocked menu in 3-4 weeks, maybe sooner. All orders placed with me will still get full attention. Awaiting orders will be sent on time. I do not intend

on answering many messages from people without orders during my restocking period. Thanks everyone for always being awesome. The empathogen crowd is legendary." Subsequently, all of the "for sale" listings on the "INSTRUMENT" profile on White House Market were taken down.

28. VOLDEN and WHEELER returned to Minnesota on June 23, 2021. Investigators on surveillance observed them being picked up at the Minneapolis St. Paul airport and being driven home to 4733 Bouleau Road, White Bear Lake, Minnesota. The following day, the "INSTRUMENT" vendor profile on White House Market was updated again stating, "I'm slowly opening listings. Shipping will resume Saturday, June 26th. I have a handful of messages to catch up on. Please be patient. Thank you!

29. On July 14, 2021, at approximately 2:00 AM investigators made two (2) separate UC purchases from "INSTRUMENT" on the dark web marketplace "White House Market". One order was for 450 milligrams of MDMA, and the other was for five (5) dosage units of LSD. A request was made to "INSTRUMENT" to combine the orders if possible in one package to save on shipping costs. The address and name provided to "INSTRUMENT" to mail the order to was Brandon Walker, P.O. Box 92, Hilliard, Ohio 43026. On July 14, 2021, at approximately 4:29 PM investigators in Minnesota observed a 2013 blue Dodge Avenger (registration plate 415RCE) known to be utilized by VOLDEN leave his residence located at 4733 Bouleau Road, White Bear Lake, MN. Investigators were able to follow the vehicle to a United States Post Office located at 1056 Highway 96 East, Saint Paul, MN, where the vehicle drove to the area of the blue USPS collection box located in the parking lot. The blue Dodge Avenger promptly left the parking lot after driving past the collection boxes, at which time investigators identified the driver as being VOLDEN. VOLDEN drove directly back to his residence on Bouleau Road after leaving the Post Office. Investigators were assisted by USPS employees to open the collection

boxes and recovered nine (9) letters similar in appearance to letters send by VOLDEN during previous UC purchases. One of the letters was addressed to Brandon Walker, P.O. Box 92, Hilliard, Ohio 43026, which was seized by the investigators. The investigators opened the letter at the DEA Minneapolis District Office, and found it to contain two separate foil like pouches. On pouch contained a small plastic zip lock baggie with brown granular substance inside which subsequently tested positive for MDMA using a field test kit, and the other pouch contained a piece of perforated paper, which subsequently tested positive for LSD.

30. On July 23, 2021, a search warrant was obtained for VOLDEN's residence located at 4733 Bouleau Road, White Bear Lake, MN. An arrest warrant for VOLDEN was also obtained. On July 27, 2021, members of the DEA Minneapolis District Office (MDO), assisted by members of COCDTF executed the search warrant and arrest warrant at VOLDEN's residence. Once in custody VOLDEN was read the Constitutional Rights Waiver (Miranda Warning) and agreed to answer questions. VOLDEN admitted to selling narcotics under the moniker INSTRUMENT on the dark web site White House Market, and shipping the narcotics throughout the United States, and internationally using the United States Postal Service. VOLDEN also admitted to having a large amount of cryptocurrency in his possession that he stated was from the sales of narcotics on the dark web. VOLDEN admitted he was not currently employed, and was living off of the proceeds from the narcotics sales. When asked how he purchased his residence VOLDEN stated he obtained a loan from BlockFi (Lending LLC), and had used the U.S. currency from the load to pay for the residence. VOLDEN went on to explain that he had used Bitcoin (BTC) as the collateral for the loan from BlockFi, and was making payments back to BlockFi to satisfy the loan. VOLDEN also admitted all of the BTC transferred to BlockFi as collateral for the loan were proceeds from his sales of illegal narcotics on the dark web.

31. Records were obtained from BlockFi Lending LLC for VOLDEN's account. The records indicated that VOLDEN had deposited approximately 37 BTC into the BlockFi account initially as collateral for the loan. Documents were also included in the records, which outlined the terms of the loan to VOLDEN. After VOLDEN's arrest members of COCDTF contacted BlockFi concerning the cryptocurrency in VOLDEN's account. Due to VOLDEN being out of compliance with the loan agreement BlockFi foreclosed on the loan, and after accounting for all funds due to them found that there were **24.06161087 BTC** left in the account that were VOLDEN's.

LAUNDERING OF NARCOTICS PROCEEDS AND ANALYSIS OF CRYPTOCURRENCY INTO THE SUBJECT ACCOUNT

32. Transactions on DWMs such as those described in this affidavit are conducted through the use of cryptocurrency, primarily Bitcoin, in order to facilitate anonymity. Proceeds from transactions on DWMs are deposited to a common wallet within the DWM known as a "hot wallet," and available balances are tracked within each user account. When a vendor wants to withdraw funds from the DWM, he/she withdraws Bitcoin from his/her DWM "account" to a Bitcoin address within his/her control. Bitcoin from the hot wallet is then transferred to the address indicated by the vendor. These financial transactions, conducted with the proceeds of illegal narcotics sales, were executed with the knowledge that it would conceal the nature, source, and origin, of such proceeds, constituting money laundering transactions under 18 U.S.C. § 1956.

33. To obtain fiat value from cryptocurrency, it must be exchanged from Bitcoin to the individual's fiat currency of choice (e.g., USD, GBP, or some denomination). This transformation of value occurs at cryptocurrency exchanges, such as Celsius, Binance, Kraken, BlockFi, or other like exchanges, which are money services businesses (MSBs). In order to use an exchange, an individual must create an account at the exchange and then send

Bitcoin, or other form of cryptocurrency, from an address they control to an address associated with their account at the cryptocurrency exchange. The individual could then withdraw funds from the cryptocurrency exchange to their bank of choice; alternately, it could be exchanged for other forms of cryptocurrency (e.g., Ethereum, Litecoin, etc.). Conducting financial transactions with the proceeds of illegal narcotics sales with the knowledge that it would conceal their nature, source, and origin, e.g., converting pseudonymous bitcoin proceeds into seemingly legitimate fiat currency, constitutes money laundering under 18 U.S.C. § 1956.

34. Because of the nature of how bitcoin is transferred between addresses, tracing a bitcoin transaction is akin to tracking a serialized dollar through the financial system. As a result, it is impractical to employ traditional tracing methods to complex, multi-hop bitcoin transactions. Instead, bitcoin flow analysis shows the overall path of where bitcoin came from prior to reaching a certain wallet or address. So, while the activity may not be directly traceable at the transactional level, it can often be indirectly traced back to an origin wallet or address. Because every bitcoin transaction is entered into the public blockchain ledger, investigators can use historical blockchain analysis to determine which origin wallets belong to bitcoin addresses well-known to law enforcement, such as DWMs (e.g., Silk Road 1, Hansa, etc.), exchanges (e.g., Celsius, Binance, Kraken, BlockFi, etc.), or peer-to-peer exchange platforms (e.g., LocalBitcoins). Wallets and addresses that belong to unknown individuals, however, are far more difficult to identify.

35. After conducting blockchain analysis, investigators believe all the self-hosted wallet clusters identified below are controlled by Christopher VOLDEN. Most funds deposited to the wallet clusters originated from the following: darknet market accounts

created by Christopher VOLDEN, Christopher VOLDEN's accounts at regulated exchanges, or mixing services previously used by Christopher VOLDEN to transfer funds. Additionally, a portion of the funds spent from the wallet clusters were ultimately deposited into Christopher VOLDEN's exchange account at BlockFi

36. On July 27, 2021 a Federal search warrant was served at VOLDEN's residence. At that time VOLDEN was also arrested on a Federal arrest warrant. VOLDEN was read the Constitutional Rights Waiver (Miranda warnings), and he agreed to answer questions. VOLDEN admitted to selling illegal narcotics on the dark web market (DWM) site White House Market (WHM) under the moniker INSTRUMENT, and shipping the illegal narcotics to customers across the United States and Internationally. VOLDEN stated he had been selling illegal narcotics on the DWM's since 2013. VOLDEN went on to state he had not had a real source of income since 2013 other than the proceeds from his sales of illegal narcotics. VOLDEN further explained that the proceeds from his DWM sales were mostly stored in cryptocurrency to include Monero (XMR), and Bitcoin (BTC).

37. When asked about the purchase of his residence located at 4733 Bouleau Road, White Bear Lake, MN, VOLDEN said he had purchased the residence in March 2021. VOLDEN explained he had transferred BTC from his wallets to his account at BlockFi as collateral. VOLDEN admitted that all of the BTC sent to the BlockFi account came from a wallet where he stored his funds from the illegal sales of narcotics on the DWM's. VOLDEN explained the BTC was used as collateral for a cash loan from BlockFi, and that he had used the U.S. currency from the loan to purchase the residence. VOLDEN went on to explain he was in the process of paying back the loan in order to regain control of the BTC he had

transferred to BlockFi as collateral for the loan, and that the funds used to repay the load had also come from the sale of illegal narcotics on the DWM's.

38. During a search of VOLDEN's Gmail account information documents were discovered between VOLDEN and BlockFi detailing the conditions of the loan. The documents also detailed the amount of collateral to be posted by VOLDEN to secure the loan, and the conditions for paying off the loan. Investigators contacted BlockFi about the status of the loan to VOLDEN. BlockFi indicated due to VOLDEN's arrest and incarceration that he was in breach of contract for the loan, and that they would be closing the account. BlockFi notified the investigators that after the final accounting of the loan and collateral that 24.06161087 BTC remained in the account, which still belonged to VOLDEN. The BTC were the total of the "over" collateral BTC that VOLDEN submitted to BlockFi in order to secure the loan.

39. Very few, if any, of the products/services being sold on DWMs are legal (e.g., contraband such as heroin) or are being sold legally (e.g., illegal sales of prescription drugs). Therefore, bitcoins being withdrawn from the DWM's represents proceeds of illegal activity in nearly every instance. Because the bitcoins being withdrawn from the DWM's consist almost entirely of criminal proceeds, I submit there is probable cause to seize the 24.06161087 BTC remaining in VOLDEN's BlockFi account.

SEALING REQUEST

40. It is respectfully requested that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested seizure warrant, including the application, this affidavit, and the requested search warrant. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing

investigation. Premature disclosure of the contents of the application, this affidavit, and the requested seizure warrant may adversely affect the integrity of the investigation, including giving VOLDEN a chance to destroy evidence or take other steps to hinder the investigation. Furthermore, because of the confidential nature of law enforcement analysis techniques disclosed herein, sealing is critical. Dark web vendors and other criminals in the dark web space frequently search the internet for legal process that describes current law enforcement techniques for tracing cryptocurrency and identifying dark web vendors. As a result, sealing this request is critical for countless ongoing investigations around the country.

TFO

Task Force Officer Andrew Wuertz
Drug Enforcement Administration

Sworn to before me on
September _____, 2021

September 1, 2021

Kimberly A. Johnson
United States Magistrate Judge